

What is claimed is:

1. A method comprising

receiving a certification message generated by a physical token of a computing

5 device that attests to a public key associated with a virtual token of the computing
device and the physical token; and

requesting an entity to issue a credential for the public key associated with the
virtual token based upon the certification message.

10 2. The method of claim 1 wherein receiving comprises

receiving the certification message that is encrypted by a public key of the entity
and that comprises a hash of both the public key associated with the virtual token and a
credential issued to the physical token.

15 3. The method of claim 2 wherein requesting comprises

sending to the entity the certification message, the public key associated with the
virtual token, and the credential issued to the physical token.

4. The method of claim 3 wherein requesting further comprises

20 sending to the entity one or more integrity metric quotes from the physical token
and one or more logs associated with the integrity metric quotes.

5. The method of claim 1 further comprising

- encrypting one or more integrity metric quotes with a session key of a symmetric cryptographic algorithm to obtain a first encrypted parameter;
- 5 encrypting the certification message and session key with a public key associated with the entity to obtain a second encrypted parameter;
- 5 wherein requesting comprises sending to the entity the first encrypted parameter and the second encrypted parameter.

6. The method of claim 1 wherein receiving comprises

10 receiving the certification message encrypted by the public key of the entity, the certification message comprising a hash that attests to the public key associated with the virtual token and a credential issued to the physical token.

7. The method of claim 1 wherein receiving comprises

15 receiving the certification message encrypted by the public key of the entity, the certification message comprising the public key associated with the virtual token and a credential issued to the physical token.

8. A physical token for a computing device, comprising

20 a register to record an integrity metric that measures a virtual token of the computing device, and

one or more processing units to generate a random number and a certification message that specifies the register, that is encrypted by a key of an entity, and that has uniqueness based upon the random number.

9. The physical token of claim 8 wherein
the one or more processing units generates the certification message such that
the certification message further comprises a hash that identifies a key associated with
5 the virtual token and a credential issued to the physical token.
10. The physical token of claim 8 wherein
the one or more processing units generates the certification message such that
the certification message further identifies a key associated with the virtual token and a
credential issued to the physical token.
11. The physical token of claim 8 wherein
the integrity metric comprises a hash of a virtual machine monitor that comprises
the virtual token.
12. The physical token of claim 8 wherein
the certification message comprises one or more hashes that attest to a key
associated with the virtual token, the credential issued to the physical token, and an
index specifying the register.
13. A computing device comprising
a virtual token to record integrity metrics;

- a physical token to record an integrity metric that measures the virtual token, and to generate a certification message that attests to the integrity metric, that is encrypted by an asymmetric key of an entity, and that has uniqueness; and
- 5 a processor to request the entity to issue a credential for an asymmetric key associated with the virtual token based upon the certification message.

14. The computing device of claim 13 wherein

the physical token generates the certification message such that the certification message that identifies the asymmetric key associated with the virtual token and a credential issued to the physical token, and

the processor sends the entity the certification message, the asymmetric key associated with the virtual token, and the credential issued to the physical token.

15. The computing device of claim 14 wherein

the processor further sends one or more integrity metric quotes from the physical token and one or more logs associated with the integrity metric quotes.

16. The computing device of claim 13 wherein the processor

sends the entity a symmetric key that is encrypted with the asymmetric key of the entity, and

sends the entity the certification message, the asymmetric key associated with the virtual token, and the credential issued to the physical token that are encrypted with the symmetric key.

17. A computing device comprising

a physical token to generate a certification message that attests to an operating environment of the computing device and a credential issued to the physical token; and

5 a virtual machine monitor comprising a virtual token to further attest to the operating environment, wherein the virtual machine monitor requests the physical token to provide the certification message, causes the certification message to be transferred to an entity, and receives a credential for the virtual token in response to transferring the certification message to the entity.

18. The computing device of claim 17 wherein

the physical token generates the certification message such that the certification message further comprises one or more hashes that identify a public key associated with the virtual token and the credential issued to the physical token.

19. The computing device of claim 17 wherein

the physical token generates the certification message such that the certification message further comprises a public key associated with the virtual token and the credential issued to the physical token.

20

20. The computing device of claim 17 wherein

the physical token generates the certification message to include an integrity metric representative of the virtual machine monitor.

21. The computing device of claim 17 wherein
the physical token and virtual token attest to the operating environment by
providing quotes of recorded integrity metrics, and
5 the virtual machine monitor further provides the entity with one or more quotes of
recorded integrity metrics.

22. A method comprising
10 receiving a request for a credential to be issued to a virtual token of a computing
device;
determining whether the virtual token satisfies criteria for a suitable virtual token
based upon information of the request; and
issuing the credential to the virtual token of the computing device in response to
determining that the virtual token satisfies the criteria.
15

23. The method of claim 22 wherein determining comprises
analyzing a credential provided by the request that was issued to a physical
token of the computing device.
20 24. The method of claim 23 wherein determining further comprises
analyzing an integrity metric representative of the virtual token of the computing
device.

- 10
15
20
25. The method of claim 24 wherein determining further comprises
analyzing an integrity metric that is based upon a hash of a monitor that
comprises the virtual token.
- 5 26. A machine readable medium comprising instructions, which in response to being
executed, result in a computing device
generating a certification message that attests to a physical token and an
operating environment of a computing device; and
requesting that an entity issue a credential to a virtual token of the computing
device based upon the certification message.
27. The machine readable medium of claim 26 wherein the instructions, in response to
being executed, further result in the computing device
generating the certification message such that the certification message
comprises a hash that attests to a public key associated with the virtual token.
28. The machine readable medium of claim 27 wherein the instructions, in response to
being executed, further result in the computing device
generating the certification message such that the certification message is
20 encrypted by a public key of the entity and the hash further attests to a credential
issued to the physical token.

29. The machine readable medium of claim 28 wherein the instructions, in response to being executed, further result in the computing device

sending the public key associated with the virtual token and the credential associated with the physical token.

5

30. The machine readable medium of claim 26 wherein the instructions, in response to being executed, further result in the computing device

generating the certification message such that the certification message is encrypted with a public key of the entity and comprises one or more hashes that attest to a public key associated with the virtual token and the credential associated with the physical token;

encrypting the public key associated with the virtual token, the credential associated with the physical tokens, the certification message, quotes of integrity metrics recorded by the physical token, and logs associated with the integrity metrics with a session key to obtain a first parameter; and

encrypting the session key with the public key of the entity to obtain a second parameter,

wherein requesting comprises sending the entity the first parameter and the second parameter.